DOCUMENT RESUME

ED 467 201 JC 020 548

| | |
|---|---|
| AUTHOR | Howard, Barbara C; Morneau, Keith A. |
| TITLE | An Innovative Community College Program and Partnership in Information Security. |
| INSTITUTION | Northern Virginia Community Coll., Annandale. |
| PUB DATE | 2002-00-00 |
| NOTE | 11p. |
| AVAILABLE FROM | For full text: http://www.nvcc.edu/home/otraksler/netsecurity/pdf/innovative.pdf. |
| PUB TYPE | Reports - Evaluative (142) |
| EDRS PRICE | EDRS Price MF01 Plus Postage. PC Not Available from EDRS |
| DESCRIPTORS | Community Colleges; *Information Technology; Program Evaluation; Program Implementation; Special Degree Programs; *Technology Education; Two Year Colleges; Vocational Education |
| IDENTIFIERS | *Northern Virginia Community College; Virginia |

ABSTRACT

This report describes an innovative network security program initiated by Northern Virginia Community College and funded with a grant from the Northern Virginia Regional Partnership. The program educates and trains students in the instillation, configuration, and troubleshooting of the hardware and software infrastructure of information security. The curriculum was designed by a team of experts in network and Internet security in the private and public sectors and offers a unique, 1-year, full-time program that combines instruction in security skills with on-the-job experience. The program content also includes training in business and communication skills. Results are presented from an information security specialist focus group convened to validate the program curriculum and identify future trends in the field of information security. The paper concludes with a discussion of the lessons learned by program administrators a year and a half after initiating the new program. These lessons include the need for an advanced networking lab, the value of professional development for full-time and adjunct faculty, and the importance of continuous curriculum development. The results of the Information Security Specialist Focus Group are presented in the appendix. (RC)

Reproductions supplied by EDRS are the best that can be made
from the original document.

ED 467 201

# An Innovative Community College Program and Partnership in Information Security

By

**Dr. Barbara C. Howard, Dean**
**Business and Public Services**
**Northern Virginia Community College**
**Annandale Campus**

**And**

**Professor Keith A. Morneau, Program Head**
**Information Systems Technology**
**Northern Virginia Community College**
**Annandale Campus**

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN MICROFICHE AND IN ELECTRONIC MEDIA FOR ERIC COLLECTION SUBSCRIBERS ONLY, HAS BEEN GRANTED BY

B. Howard

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

2A

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☒ This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

## Introduction

In December 2000, the Annandale Campus of Northern Virginia Community College (NVCC) was awarded a grant of approximately $250,000 from the Northern Virginia Regional Partnership (NVRP) to launch a new credit, vendor-neutral certificate program in Network Security. The NVRP was a partnership between business and education that provided seed money for Information Technology (IT) workforce programs in Northern Virginia.

In the summer of 2001, several courses were piloted on the Annandale and Woodbridge campuses of NVCC. The complete seven-course program in Network Security was launched in August 2001. It has a steady-state population of 250 students. A distance-learning initiative will launch in August 2002.

The program at NVCC educates and trains students in the installation, configuration, and troubleshooting of the hardware and software infrastructure of information security. Designed by a team of experts in network and Internet security in the private and public sectors, it is a

IC020548



BEST COPY AVAILABLE

unique, one-year, full-time program that combines instruction in security skills with on-the-job experience.

The Information Security team at NVCC consists of faculty from both the Annandale and Woodbridge Campuses of Northern Virginia Community College. The Information Security Team sold the proposal to the NVRP, set up the faculty team, found industry sponsorship and support, and assigned the Project Manager to assume responsibility for the management of grant.

The companies who assisted NVCC in launching this program are ECommSecurity (content expertise), Symantec (software), and Intel (advanced networking lab). Key individuals from information technology security companies provided advice and counsel to the NVCC program.

The Institute for Excellence in Information Technology (IE-IT) in the Virginia Community College System (VCCS) offered the program to the other 23 community colleges in the state and provided funding for continued course development and professional development. The program has been adopted and adapted by four additional community colleges in Virginia: Tidewater Community College (Norfolk), New River Community College (Dublin), J. Sargent Reynolds Community College (Richmond), and Lord Fairfax Community College (Middleton). More Virginia community colleges plan to adopt the program in the future.

**Career Pathways in Information Security**

A focus group of information security professionals in the government and commercial sectors was held to validate the NVCC program in information security and to provide input for future directions of the program. The focus group talked in-depth about information security as a career path. The group came up with three distinct levels of information security professionals:

- Entry-level professionals hold positions such as Security Specialist, Information Assurance Specialist, Information Systems Security Specialist, Network Security Specialist, Applications Security Specialist, and Operating System Security Specialist. This level consists of front-line workers in the information security field and contains the greatest number of information security jobs in the marketplace. However, few professionals at this level are currently educated and trained in information security. This level is a niche area for community colleges to provide needed education and training in information security. Most information security programs today are at the post-graduate level, which trains for a higher-level job than what most employers are looking for.

- Mid-level information security professionals are security engineers with a bachelor's degree in information security.

- Senior-level information security professionals hold positions such as Security Architect, Senior Security Engineer, and Senior Security Consultant. This level corresponds to the post-graduate degree programs, as the focus group saw it. The focus group felt that most of their entry-level needs could be met from the community colleges and suggested that all information security professionals start at this level and move up the career ladder from there.

The challenge is to provide an educational pathway for security professionals that are tied to a career ladder. To make this educational pathway a reality, strong articulation agreements are needed between community colleges and four-year institutions.

The focus group wanted to see two additional components incorporated into education and training programs in information security: business skills and communication skills. The group felt that a world-class security program would consist of technical knowledge and skills, technical experiences, and business and communications skills. Appendix A contains the tasks list created by the focus group.

**Curriculum Philosophy and Design**

In the article "Clarke Warns Educators About the Need for Better Security" (*Computerworld*, June 5, 2002), Deborah Radcliff states that most information security programs focus completely on technology issues without regard to business value and skills in critical thinking. The program at NVCC is designed to provide education and training in business skills and communications skills in conjunction with technical knowledge and skills. NVCC believes that all education and training programs in IT need to provide technical knowledge and skills, value-delivery skills (business and communication skills), and technical experiences to be successful. The network-security certificate program was designed with these components in mind.

The focus group wanted students to have a strong foundation in computer networking before they were allowed to enroll in the security program. Information Systems Technology (IST) faculty decided to make its networking degrees the foundation of knowledge needed to take the information security program. NVCC's ultimate goal is to make the network-security

certificate program a degree program, either through articulation with a four-year school or by developing the certificate program into a degree program.

Currently, with almost a year of experience teaching information security to students, NVCC faculty decided to not make the certificate program a degree program at this time because of the need for students to have that strong foundation in networking. The philosophy of NVCC's information security program is to teach students foundational knowledge in information security, an attack methodology, and a defense methodology (also known as defense-in-depth) spread over six courses. Three-credit classes include theory and concepts, hands-on lab classes, and a capstone course.

The capstone course was designed to provide students with "real-world" experiences that would result in a presentation and a portfolio of work that could be shown to potential employers. The capstone course was taught for the first time in the spring semester of 2002 and was a huge success. Students worked in teams of three or four, developed an attack plan, executed the attack plan (they do not penetrate any network), provided a vulnerability analysis to companies, and presented the findings to a network-security panel that consisted of faculty and industry representatives. The future of this course is to provide vulnerability analysis to non-profit corporations in the Washington, D.C., and metropolitan area.

**Lessons Learned**

IST faculty has learned many lessons in more than a year and a half of successfully teaching information security at the community college level. One of the lessons learned is the need for an advanced networking lab to support this kind of program. The initial lab cost roughly $90K, which includes both hardware and software. Fortunately, much open source

software is available that can be used free of charge. In addition, the maintenance expense is needed to keep the lab up and running is substantial. This lab must be isolated from the Internet during class and during labs. NVCC uses hacking software to demonstrate attack methodologies being currently used. NVCC faculty and staff decided that the lab would not be connected to the Internet for ethical reasons.

The importance of professional development of full-time and adjunct faculty is another lesson learned. Faculty who teach in this program must have a strong background in networking and in TCP/IP. NVCC concluded that someone needed to have experience in teaching networking and in TCP/IP to be an ideal candidate to teach in this program. Full-time faculty must attend professional development seminars, workshops, and courses. NVCC recommends SANS and Learning Tree International as training sources. NVCC also recommends that faculty attend SANS conferences to get the most up-to-date knowledge. NVCC spent well over $30K on faculty professional development in the beginning of the program.

A third lesson learned is the importance of continuous curriculum development. Faculty must be paid stipends to keep the content in the curriculum up-to-date. An on-going effort is needed to improve the program and tweak the content once it has been taught. This requires a considerable amount of development time to perform. Virginia decided that this program was important enough to dedicate funds for faculty stipends throughout the year to keep the program up-to-date. NVCC faculty has worked over 1000 hours to develop and maintain this program to date.

**Conclusion**

In response to the growing needs of business and industry, NVCC introduced a new Network Security Certificate in August of 2001. This unique, vendor-neutral, one-year program teaches students to install, configure, and troubleshoot the hardware and software of security infrastructure. By offering instruction in security, business, and communication skills and technical experience in the information security area, the program will thoroughly prepare students to fill a position in the rapidly growing field of information security.

The NVCC program was designed by network and Internet security experts in the private and public sectors and consists of three three-credit theory courses, three three-credit lab courses, and a capstone course. The program is currently offered on the Annandale and Woodbridge campuses. The Manassas and Alexandria campuses offer courses in the program, but not the full program. Currently, NVCC has 250 students enrolled and just graduated its first four students in May of 2002.

## Appendix A: Information Security Specialist Focus Group Results

Duty Area 1: Understanding the Importance of Security for a Business

1.1. Identify financial implications of information security for a business.
1.2. Identify physical implications of information security for a business.
1.3. Identify personnel and administrative implications of information security for a business.
1.4. Identify legal implications of information security for a business.
1.5. Identify customer service implications of information security for a business.
1.6. Identify physical security measures and explain their importance.

Duty Area 2: Understanding Network Hardware, Network Protocols, and Computer Operating Systems

2.1 Demonstrate a strong system level knowledge of network hardware.
2.2 Demonstrate a strong system level knowledge of network protocols.
2.3 Demonstrate a strong system level knowledge of computer operating systems.

Duty Area 3: Understanding Security Management

3.1. Understand the importance of and implement security policies and procedures.
3.2. Understand the importance of and implement security audits and assessments.
3.3. Understand the differences between operations security and information security.
3.4. Identify the basic role of cryptography in information security.

Duty Area 4: Understanding the Ever-widening Scope of Security Risk

4.1. Identify capabilities and limitations of various communications systems—e.g., microwave, satellite, wireless technology—and their implications for security risk.
4.2. Identify the various information media subject to security risk (e.g., audio, video, data).
4.3. Identify the variety of products and systems involved in information security (e.g., Intrusion Detection Systems (IDS), anti-virus software, firewalls).
4.4. Compare and contrast the types and implications of security risks for private and public sectors.

Duty Area 5: Managing Security Protection

5.1. Install, configure, and manage operating system-specific security (e.g., Novell, Microsoft, Unix, Linux).
5.2. Install, configure, and manage application-specific security (e.g., for e-mail, database management, web browser).
5.3. Install, configure, and manage telecommunications and network hardware security (e.g., ISO/OSI layers, firewalls, routers, switches, gateways, proxies).
5.4. Manage protocols.
5.5. Install, configure, and manage encryption measures (e.g., PKI).
5.6. Install, configure, and manage IDS products.
5.7. Install, configure, and manage anti-virus software.
5.8. Secure servers (e.g., web server, mail server, DNS server).
5.9. Install, configure, and manage virtual private network (VPN).
5.10. Implement privilege management procedures (identification and authentication - I&A).

Duty Area 6: Detecting Vulnerability and Breaches

6.1. Understand the importance and purposes of vulnerability analysis/ penetration testing.
6.2. Run vulnerability/scanning tools against networks and computers.
6.3. Analyze/report findings of vulnerability analyses.
6.4. Identify objectives of attackers (e.g., destruction of data, compromise of data, corruption of application or system, exposure of vulnerability).
6.5. Explain the difference among event, incident, and investigation.
6.6. Understand malicious codes.
6.7. Understand jargon (e.g., hackers, crackers, phreaks, script kiddies, white hat/black hat).
6.8. Identify types of attacks (e.g., denial of service, virus, hacking).
6.9. Monitor system log files.
6.10. Locate security breach.
6.11. Determine type and extent of damage.

Duty Area 7: Responding to Security Threats and Breaches

7.1. Respond to general threat (e.g., announcements of virus threat; manufacturers' security alerts).
7.2. Respond to warnings from anti-virus software.
7.3. Identify sources of information for security patches.
7.4. Acquire and install security patches.
7.5. Secure web browser or apply other fix as response to specific breach.
7.6. Implement crisis management procedures.
7.7. Implement disaster recovery procedures.

Duty Area 8: Using Communication Skills in the Workplace

8.1. Communicate correctly, clearly, and concisely in speech and in writing.
8.2. Participate as a team member (e.g., Incident Response Team) to accomplish goals.
8.3. Follow instructions.
8.4. Document protective, detective, and corrective measures taken (e.g., analyses, recommendations, warnings, incidents, actions).
8.5. Explain security issues to coworkers.
8.6. Answer questions about computer security.
8.7. Locate and interpret information (e.g., corporate business guidelines, best business practices, manufacturers' user guides).

Duty Area 9: Understanding the Legal and Ethical Implications of Security

9.1. Examine basic security-related civil law (e.g., privacy, freedom of speech).
9.2. Examine basic security-related criminal law (theft, fraud, etc.).
9.3. Identify the role of basic forensics in information security.
9.4. Examine ethical issues related to security (e.g., those related to privacy of data).

Duty Area 10: Ensuring Professional Development

10.1. Explain the types and purposes of information security certification.
10.2. Explain the importance of continuing education for information security professionals.
10.3. Identify trends in the field.

10.4. Explain ways an information security professional can stay abreast of techniques and technologies in the field.

Duty Area 11: Completing the Capstone Exercise

11.1. Evaluate given situation.
11.2. Recommend or implement appropriate security response.
11.3. Present findings and responses in a professional manner.

**U.S. Department of Education**
*Office of Educational Research and Improvement (OERI)*
*National Library of Education (NLE)*
*Educational Resources Information Center (ERIC)*

ERIC

# REPRODUCTION RELEASE

(Specific Document)

## I. DOCUMENT IDENTIFICATION:

| | |
|---|---|
| Title: An Innovative Community College Program and Partnership in Information Security | |
| Author(s): Dr. Barbara C. Howard and Professor Keith Morneau | |
| Corporate Source: Northern Virginia Community College | Publication Date: July 2002 |

## II. REPRODUCTION RELEASE:

In order to disseminate as widely as possible timely and significant materials of interest to the educational community, documents announced in the monthly abstract journal of the ERIC system, *Resources in Education* (RIE), are usually made available to users in microfiche, reproduced paper copy, and electronic media, and sold through the ERIC Document Reproduction Service (EDRS). Credit is given to the source of each document, and, if reproduction release is granted, one of the following notices is affixed to the document.

If permission is granted to reproduce and disseminate the identified document, please CHECK ONE of the following three options and sign at the bottom of the page.

The sample sticker shown below will be affixed to all Level 1 documents

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY

Sample

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

1

Level 1

☐

Check here for Level 1 release, permitting reproduction and dissemination in microfiche or other ERIC archival media (e.g., electronic) and paper copy.

The sample sticker shown below will be affixed to all Level 2A documents

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN MICROFICHE, AND IN ELECTRONIC MEDIA FOR ERIC COLLECTION SUBSCRIBERS ONLY, HAS BEEN GRANTED BY

Sample

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

2A

Level 2A

☒

Check here for Level 2A release, permitting reproduction and dissemination in microfiche and in electronic media for ERIC archival collection subscribers only

The sample sticker shown below will be affixed to all Level 2B documents

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN MICROFICHE ONLY HAS BEEN GRANTED BY

Sample

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

2B

Level 2B

☐

Check here for Level 2B release, permitting reproduction and dissemination in microfiche only

Documents will be processed as indicated provided reproduction quality permits.
If permission to reproduce is granted, but no box is checked, documents will be processed at Level 1.

*I hereby grant to the Educational Resources Information Center (ERIC) nonexclusive permission to reproduce and disseminate this document as indicated above. Reproduction from the ERIC microfiche or electronic media by persons other than ERIC employees and its system contractors requires permission from the copyright holder. Exception is made for non-profit reproduction by libraries and other service agencies to satisfy information needs of educators in response to discrete inquiries.*

| | | |
|---|---|---|
| *Sign here, → please* | Signature: Barbara C. Howard | Printed Name/Position/Title: Dr. Barbara C. Howard, Dean, Business and Public Services |
| | Organization/Address: Northern Virginia Community College<br>8333 Little River Turnpike<br>~~Annendale, VA 22003~~ | Telephone: 703.323.3157 FAX: 703.323.3015<br>E-Mail Address: bhoward@nvcc.vccs.edu Date: July 23, 2002 |